UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF WISCONSIN

UNITED STATES OF AMERICA, Case No. 15-CR-216-PP

Plaintiff,

v.

JAMES G. WHEELER,

Defendant.

DECISION AND ORDER DENYING DEFENDANT'S MOTION TO SUPPRESS EVIDENCE (DKT. NO. 9)

On November 3, 2015, defendant Wheeler was indicted by a federal grand jury on charges of violating the Hobbs Act (18 U.S.C. §§1951(a) and (2)) by robbing an employee of a clothing store by means of force, and of knowingly using, carrying or brandishing a firearm during and in relation to a crime of violence, in violation of 18 U.S.C. §§924(c)(1)(A)(iii) and 2. Dkt. No. 1. On December 4, 2015, the defendant filed a motion to suppress cell site information. Dkt. No. 9. The motion asked the court to suppress "all data disclosed by Sprint Corporation to the government regarding cell tower information from a cellular telephone," because "obtaining this information was a 'search' for purposes of the Fourth Amendment, and may only be searched if the government obtains a warrant that is supported by probable cause." Id. at 1. Specifically, the defendant challenged the Stored Communications Act, 18 U.S.C. §2703(d) ("SCA"), which allows the government to obtain an order for such information by simply establishing reasonable grounds to believe that the

information to be obtained would be relevant and material to an investigation. The defendant asked the court to find that §2703(d) is unconstitutional as applied to the facts in his case. Id. at 1-2.

The government responded to the motion to suppress on December 14, 2015, Dkt. No. 11, and Magistrate Judge David E. Jones issued a recommendation on January 6, 2016, Dkt. No. 15. Judge Jones first noted that the Seventh Circuit had not decided whether cell users had a Fourth Amendment reasonable expectation of privacy in historical cell site location data. Id. at 6. He pointed to several courts, including one magistrate judge in this district, which had concluded that such an expectation of privacy was not reasonable, id. at 6-7, opining that "most federal judges" had decided the issue that way, id. at 7. Judge Jones acknowledged that the defendant had asked him to follow a Fourth Circuit decision to the contrary, but declined to take up the Fourth Amendment issue. Id. at 8. Instead, he concluded that the good-faith exception to the exclusionary rule applied, and mandated denial of the suppression motion. Id. at 8-10. Judge Jones recommended that this court deny the motion to suppress. Id. at 11.

The defendant has objected to Judge Jones' recommendation. Dkt. No. 17. The objection specifically asked this court to reach the question of whether the government most seek a warrant in order to obtain cell site location data from a provider. Id. at 4. The defendant argues that providers received thousands of cell site location data requests from law enforcement in 2014 and 2015, and noted that the United States Supreme Court had advised lower

courts to address the merits of Fourth Amendment claims "when necessary to guide future action by law enforcement and magistrates." Id. at 4 (citing United States v. Leon, 468 U.S. 897, 924 (1984).

While this court agrees with Magistrate Judge Jones' determination that the good-faith exception to the exclusionary rule applies in this case, the court will grant the defendant's request to consider the merits of the Fourth Amendment argument. The Seventh Circuit has declined one request to address this specific issue precisely because no party raised it in the district court. See United States v. Daniels, 803 F.3d 335, 351 (7th Cir. 2015). The statistics the defendant cites in his objection indicate that law enforcement frequently make use of SCA orders to obtain cell site location data. The court agrees with the defendant that this issue is likely to re-occur in this district. For that reason, this decision considers only the Fourth Amendment question, and the court finds that collecting cell site location data does not constitute a search under that amendment.

Background

On October 7, 2015, the government applied for an order under §2703(d), asking Sprint to disclose records regarding cell phone number (414) 366-5233. Dkt. No. 9 at 2. Among the records the government requested were "[a]ll data about which 'cell towers' (i.e., antenna towers covering geographic areas) and 'sectors' (i.e., faces of the towers) received a radio signal from each cellular telephone or device assigned to the account." Id. The government based its request on information it received from an informant who had told the

government that he'd participated in a robbery with the defendant, and that the defendant had used that telephone on the day of the robbery. The government hoped the data it sought from Sprint would allow it to identify and locate the defendant. Id. The magistrate judge to whom the application was addressed granted that request, and the defendant argued in the motion to suppress that the government intends to use the data it obtained pursuant to that order if the case goes to trial.[1] Id. at 3.

The Stored Communications Act

The SCA allows the government to require an electronic communications provider to provide it with records or information "pertaining to a subscriber to or a customer of such service (not including the contents of communications)" if the government either "obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure" or "obtains a court order for such disclosure under subsection (d) of this section." 18 U.S.C. §§2703(c)(A) and (B). Subsection (d) reads as follows:

> **(d) Requirements for court order.**—A court order for disclosure under subsection (b) or (c) may be issued by any court that is a court of competent jurisdiction and shall issue only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation. . . .

[1] Footnote 1 in the motion to suppress indicates that the government informed the defendant that it intended to use only the cell tower information it obtained, not other information that Sprint disclosed as a result of the magistrate judge's order. Thus, Judge Jones considered only the challenge to the cell tower information; the defendant has reserved the right to move to suppress any other Sprint information the government may later attempt to introduce at trial. Dkt. No. 9 at 3 n.1.

The defendant has conceded that in this case, the government's application met the "reasonable grounds" standard articulated in §2703(d). The motion to suppress argued, however, that under the circumstances of this case, the Fourth Amendment required the government to obtain a warrant in order to obtain the cell tower information. Dkt. No. 9 at 6.

The Defendant's Objection

The defendant has pointed out that three federal appellate courts—the Eleventh, the Fifth and the Fourth Circuits—have ruled on the question of whether "cell tower information that telecommunication carriers collect is protected by the Fourth Amendment." Id. (quoting Daniels, 803 F.3d at 351 (declining to decide the issue because the defendant failed to raise it in the district court)). The Seventh Circuit has not decided the issue. The Eleventh Circuit and the Fifth Circuit have held that obtaining cell site data from a third-party provider does not constitute a "search" or "seizure" under the Fourth Amendment. United States v. Davis, 785 F.3d 498, 511 (11th Cir. 2015) (*en banc*); In re United States for Historical Cell Site Data, 724 F.3d 600, 611-13 (5th Cir. 2013). A panel of the Fourth Circuit, in an appeal calendared for *en banc* rehearing,[2] decided otherwise. United States v. Graham, 796 F.3d 332 (4th Cir. 2015), reh'g en banc granted, 624 F. App'x 75 (4th Cir. Oct. 28, 2015).

[2] The order granting *en banc* review indicates that the case is "tentatively calendared for oral argument during the court's March 22-25, 2016, oral argument session." United States v. Graham, 624 F. App'x 75 (4th Cir. Oct. 28, 2015).

In his objection to Judge Jones' recommendation, the defendant argued that Judge Jones "did not address whether obtaining [cell site location information] requires a warrant based on probable cause." Dkt. No. 17 at 3. Rather, the defendant argues, Judge Jones did not reach that issue, because he concluded that the good-faith exception to the exclusionary rule applied (the government having relied upon the validity of the procedures Congress had laid out in the SCA). Id. The defendant asks this court to reach the question of whether the government's collection of cell site location data from a third-party provider constitutes a "search" that requires a warrant, and he relies on the motion he filed before Judge Jones in arguing that the court should conclude that such activity does constitute a search under the Fourth Amendment, and does require a warrant. Id. at 4. In the motion filed with Judge Jones, the defendant relied almost exclusively on the Fourth Circuit's decision in United States v. Graham. Dkt. No. 9 at 3-16.

The Three Circuit Court Decisions

The Fifth Circuit

In 2013, a panel of the Fifth Circuit reviewed a district court's decision that the "SCA violates the Fourth Amendment because the Act allows the United States to obtain a court order compelling a cell phone company to disclose historical cell site records merely based on a showing of 'specific and articulable facts,' rather than probable cause." In re U.S. for Historical Cell Site Data, 724 F.3d 600, 605-606 (5th Cir. 2013) (citations omitted). In considering whether an order requiring a provider to disclose cell phone data constituted a

"search" or "seizure," the Fifth Circuit began by noting that "[t]his question of *who* is recording an individual's information initially is key . . . ." Id. at 610. Why? Because

> the individual must occasionally transact business with other people. When he does so, he leaves behind, as evidence of his activity, the records and recollections of others. He cannot expect that these activities are his private affair. To the extent an individual knowingly exposes his activities to third parties, he surrenders Fourth Amendment protections, and, if the Government is subsequently called upon to investigate his activities for possible violations of the law, it is free to seek out these third parties, to inspect their records, and to probe their recollections for evidence.

Id. (quoting Reporters Comm. for Freedom of Press v. Am. Tel. & Tel. Co., 593 F.2d 1030, 1043 (D.C. Cir. 1978) (alteration omitted)). Based on this reasoning, the Fifth Circuit concluded that "cell site information is clearly a business record," and that "[t]he cell provider collects and stores historical cell site data for its own business purposes . . . ." Id. at 611. That court noted that "[t]he Government does not require service providers to record this information or store it. The providers control what they record and how long these records are retained." Id. at 612. Given that, the court concluded that "the Government merely comes in after the fact and asks a provider to turn over records the provider has already created." Id. at 612.

With regard to a cell phone user's expectation of privacy, the Fifth Circuit reasoned that "[a] cell service subscriber, like a telephone user, understands that his cell phone must send a signal to a nearby cell tower in order to wirelessly connect his call." Id. at 613. The court also concluded that cell phone users' "use of their phones . . . is entirely voluntary." Id. (citing United

States v. Skinner, 690 F.3d 772, 777 (6th Cir. 2012)). Finally, while acknowledging that advancing technology might be changing citizens' expectations of privacy, the court stated that "[i]n circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative. A legislative body is well situated to gauge changing public attitudes, to draw detailed lines, and to balance privacy and public safety in a comprehensive way." Id. at 614 (quoting United States v. Jones, ____ U.S. _____, 132 S. Ct. 945, 964 (2012)). The court acknowledged that:

> cell phone users may reasonably want their location information to remain private, just as they may want their trash, placed curbside in opaque bags, or the view of their property from 400 feet above the ground, to remain so. But the recourse for these desires is in the market or the political process: in demanding that service providers do away with such records (or anonymize them) or in lobbying representatives to enact statutory protections. The Fourth Amendment, safeguarded by the courts, protects only reasonable *expectations* of privacy.

Id. at 615 (citations omitted).

For these reasons, the Fifth Circuit held that Fourth Amendment precedent "does not recognize a situation where a conventional order for a third party's voluntarily created business records transforms into a Fourth Amendment search or seizure when the records cover more than some specified time period or shed light on a target's activities in an area traditionally protected from government intrusion." Id.

The Eleventh Circuit

In Davis, the Eleventh Circuit, sitting *en banc*, also concluded that "the government's obtaining a § 2703(d) court order for the production of [a cell

provider's] business records did not violate the Fourth Amendment." Davis, 785 F.3d at 511. The court first concluded that cell tower records are created, stored and controlled, not by the defendant, but by the provider, and thus that such "non-content evidence" does not belong to the defendant. Id. Second, the court concluded that the defendant did not have any "subjective or objective reasonable expectation of privacy in [the provider's] business records showing the cell tower locations that wireless connected his calls at or near the time of [his crimes]." Id. Regarding a subjective expectation of privacy, the Eleventh Circuit stated that "[u]sers are aware that cell phones do not work when they are outside the range of the provider company's cell tower network." Id. As to an objective expectation of privacy, the Eleventh Circuit found "no reason to conclude that cell phone users lack facts about the functions of cell towers or about telephone providers' recording cell tower usage." Id. (citing Smith v. Maryland, 442 U.S. 735, 742-43 (1989)). For all of these reasons, the Eleventh Circuit concluded that "the government's obtaining a § 2703(d) court order for production of [the provider's] business records at issue did not constitute a search and did not violate the Fourth Amendment rights of [the defendant]." Id. at 513.

The Fourth Circuit

The defendant urged Judge Jones, and urges this court, to follow the conclusion reached by a panel of the Fourth Circuit in United States v. Graham, 796 F.3d 332 (4th Cir. 2015), reh'g *en banc* granted, 624 F. App'x. 75

(4th Cir. Oct. 28, 2015). The court will discuss that decision in more detail in the analysis section, below.

Analysis

Supreme Court Jurisprudence

Many of the Supreme Court's search-and-seizure decisions start by analyzing the question of whether the government activity at issue constitutes and intrusion into an individual's privacy, and the spectrum of activities which may or may not constitute intrusion grows broader with every technological innovation. At one end of the spectrum, the Court's cases have adhered to an "understanding that mere visual observation does not constitute a search." United States v. Jones, 132 S. Ct. at 953 (citing Kyllo v. United States, 533 U.S. 27, 31-32 (2001)). "What a person knowingly exposes to the public . . . is not a subject of Fourth Amendment protection." Katz v. United States, 389 U.S. 347, 351-52 (1967).

At the other end of the spectrum, if the government "physically occupie[s] private property for the purpose of obtaining information," it has conducted a search. United States v. Jones, 132 S. Ct. at 949. The Jones court held that the act of installing a GPS device on a target's car (which the target owned/possessed at the time of the installation), then using that device to monitor the movements of the car, was a physical "trespass," and constituted a search. Id.

Between the two ends of the spectrum are government activities that do not constitute trespass, but allow the government to obtain information in which an individual might have a reasonable expectation of privacy.

While there appears to be little doubt that government action that involves physical trespass constitutes a search, the Court has held that government activity need not constitute a physical trespass or seizure in order to constitute a search under the Fourth Amendment. Katz, 389 U.S. at 353 (1967) (" . . . once it is recognized that the Fourth Amendment protects people—and not simply 'areas'—against unreasonable searches and seizures it becomes clear that the reach of that Amendment cannot turn upon the presence or absence of a physical intrusion into any given enclosure.") "[E]ven in the absence of trespass, 'a Fourth Amendment search occurs when the government violates a subjective expectation of privacy that society recognizes as reasonable.'" Jones, 132 S. Ct. at 954 (Sotomayor, J., concurring) (quoting Kyllo, 533 U.S. at 33). "[W]hat [a person] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected." Katz, 389 U.S. at 351-52 (citations omitted).

In assessing the growing universe of factual scenarios that do not involve physical trespass but may involve a violation of an expectation of privacy, courts must look at whether the person challenging the search "exhibited an actual (subjective) expectation of privacy," and whether that expectation was "one that society is prepared to recognize as 'reasonable.'" Id. at 361 (Harlan, J., concurring) (internal quotation marks omitted). In considering whether the

person has exhibited an expectation of privacy, the Supreme Court has looked at whether the "individual, by his conduct," has shown that "'he seeks to preserve [something] as private.'" United States v. Knotts, 460 U.S. 276, 281 (1983) (citing Katz, 389 U.S. at 351). In considering whether the expectation is a reasonable one, courts must look at whether the expectation, "viewed objectively, is 'justifiable' under the circumstances." Id. (citing Katz, 389 U.S. at 361).

The court has made clear that individuals have both a subjective and a reasonable expectation of privacy inside their homes.[3] See, e.g., Illinois v. Rodriguez, 497 U.S. 177 (1990); Payton v. New York, 445 U.S. 573 (1980); Silverman v. United States, 365 U.S. 505 (1961). Thus, when law enforcement officers, from outside of the defendant's residence, aimed a thermal imaging device at the house to detect the heat emitted by marijuana grow lamps, the Supreme Court held that "obtaining by sense-enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without physical 'intrusion into a constitutionally protected

[3] The Court has held that the same expectation of privacy, regardless of the individual's subjective expectation, is not reasonable when the area at issue is the outside of a person's home. See Florida v. Riley, 488 U.S. 445, 450-51 (1989) (officer's view of the defendant's partially-open greenhouse from a helicopter was not a search, because the defendant "could not reasonably have expected the contents of his greenhouse to be immune from examination by an officer seated in a fixed-wing aircraft flying in navigable space at an altitude of . . . 500 feet . . . ."); California v. Ciraolo, 476 U.S. 207, 215 (1986) (officer's surveillance of the defendant's yard from an airplane did not constitute a search, because "[i]n an age where private and commercial flight in the public airways is routine, it is unreasonable for respondent to expect that his marijuana plants were constitutionally protected from being observed with the naked eye from an altitude of 1,000 feet.").

area'" violated the defendant's objectively reasonable expectation of privacy regarding the interior of his home. Kyllo, 533 U.S. at 34 (quoting Silverman, 365 U.S. at 512).

Similarly, the Court held that law enforcement agents' monitoring of a "beeper" transmitter when the transmitter is inside a private residence constitutes a search. See United States v. Karo, 468 U.S. 705, 714 (1984) ("This case thus presents the question whether the monitoring of a beeper in a private residence, a location not open to visual surveillance, violates the Fourth Amendment rights of those who have a justifiable interest in the privacy of the residence. . . . [W]e think that it does.") The court came to this conclusion because "private residences are places in which the individual normally expects privacy free of governmental intrusion not authorized by a warrant, and that expectation is plainly one that society is prepared to recognize as justifiable," id. at 714, and because by monitoring the beeper, "the Government surreptitiously employ[ed] an electronic device to obtain information that it could not have obtained by observation from outside the curtilage of the house," id. at 715. Namely, the monitoring

> [t]ells the agent that a particular article is actually located at a particular time in the private residence and is in the possession of the person or persons whose residence is being watched. Even if visual surveillance has revealed that the article to which the beeper is attached has entered the house, the later monitoring not only verifies the officers' observations but also establishes that the article remains on the premises.

Id.[4]

Individuals also may, under certain circumstances, have an objectively reasonable expectation of privacy in a physical space that is not the interior of their home. In Katz, the court concluded that the government conducted a search when it attached an electronic listening device to the outside of a telephone booth, allowing it to listen to and record a person who went into a phone booth, "shut[] the door behind him, and pa[id] the toll that permit[ted] him to place a call," Katz, 389 U.S. at 352, even though the government did not physically enter the phone booth. In his concurring opinion, Justice Harlan reasoned a person in a phone booth had a subjectively reasonable expectation of privacy; once someone had entered a phone booth and closed the door behind him, the booth became "a temporarily private place whose momentary occupants' expectations of freedom from intrusion are recognized as reasonable." Id. at 361.

Once the government action moves away from gathering information about the interior of a person's home, or from some other physical space in which an individual may isolate herself from the public purview, it becomes more difficult for an individual to demonstrate that an expectation of privacy,

[4] If officers monitor a beeper inside a car traveling on "public thoroughfares," however, the individual driving the car "has no reasonable expectation of privacy in his movements from one place to another." Knotts, 460 U.S. at 281-82. The court found that under those circumstances, the monitoring of the beeper did not reveal anything that visual surveillance (given enough law enforcement agents) would not have revealed. The placement of the beeper did not constitute a physical trespass, either, because "the beeper had been placed in the container before it came into Knotts' possession, with the consent of the then-owner." Jones, 132 S. Ct. at 951.

even if subjective, is reasonable. In 1976, the Court held that using a subpoena to obtain copies of the defendant's checks and deposit slips from his bank did not constitute a search. United States v. Miller, 425 U.S. 435 (1976). The court "perceive[d] no legitimate 'expectation of privacy' in the[] contents" of the bank records, id. at 442; it concluded that the records belonged to the bank, not the defendant, id. at 440, and emphasized that

> [t]his Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed [by that third party] to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.

Id. at 443.

In Smith v. Maryland, 442 U.S. 735, 743-44 (1979), the Court reiterated that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." In Smith, the defendant argued that law enforcement's collection of information about the telephone numbers that the defendant had dialed from his landline phone, collected via a pen register installed by the phone company at law enforcement's request, constituted a search. Id. at 738-39. The Supreme Court disagreed. It first expressed "doubt that people in general entertain any actual expectation of privacy in the numbers they dial." Id. at 742. The Court opined that telephone users "realize that they must 'convey' phone numbers to the telephone company, since it is through the telephone company switching equipment that their calls are completed." Id. The Court also pointed out that phone users "realize . . . that the phone company has facilities for making permanent records of the

numbers they dial, for they see a list of their long-distance . . . calls on their monthly bills." Id. The Court went on to explain other facts which ought to give telephone users reason to know that the phone company was capable of collecting the numbers they dialed. Id.

The Court also held that even if, somehow, a phone user "did harbor some subjective expectation that the phone numbers he dialed would remain private, this expectation is not 'one that society is prepared to recognize as "reasonable."'" Id. (quoting Katz, 389 U.S. at 361) (Harlan, J., concurring). Citing its decision in Miller, the Court stated that "[t]his Court consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." Id. at 743-44. The court concluded that "[w]hen he used his phone, petitioner voluntarily conveyed numerical information to the telephone company and 'exposed' that information to its equipment in the ordinary course of business," thus "assum[ing] the risk that the company would reveal to police the numbers he dialed." Id. at 744.

This reasoning—that once an individual turns information over to a third party, the individual's expectation of privacy is no longer reasonable—has led the Court to conclude that an individual who shipped cocaine (inside a tube made of duct tape, then surrounded by newspaper, placed inside a cardboard box and wrapped in brown paper) via a private freight carrier had no reasonable expectation of privacy in the contents of the package once the original expectation of privacy had been "frustrated" by transit damage that occurred prior to law enforcement's involvement, United States v. Jacobsen,

466 U.S. 109, 126 (1984), and that residents who put their garbage out on the curb for collection have no reasonable expectation of privacy, California v. Greenwood, 486 U.S. 35, 40 (1988).

In 2014, the Supreme Court confronted a challenge to law enforcement officers' accessing of information stored in the defendant's cell phone. Riley v. California, 134 S. Ct. 2473 (2014). The Court framed the issue as follows: "The two cases before us concern the reasonableness of a warrantless search incident to a lawful arrest." Id. at 2482. In particular, the Court focused on "the extent to which officers may search property found on or near the arrestee," id. at 2483-83, and looked to its decisions in Chimel v. California, 395 U.S. 752 (1969), United States v. Robinson, 414 U.S. 218 (1973), and Arizona v. Grant, 556 U.S. 332 (2009) for guiding principles in answering whether the search-incident-to-arrest exception to the warrant requirement extended to an officer's search of the data on an arrestee's cell phone.

It does not appear from a reading of the Riley opinion that any party argued that the officers did not conduct "searches" when they accessed the data on the defendants' phones. To the contrary, the government argued that searching the data stored in a cell phone was "materially indistinguishable" from searching things like wallets, zippered bags and address books. Id. at 2488-89. Given that arrestees have "diminished privacy interests" because the grounds that give rise to the arrest and detention provide the government with a basis for intruding into the arrestee's privacy, the government argued that the diminished privacy interests occasioned by an arrest allowed officers to

search a cell phone on an arrestee's person, just as it would allow their search of a wallet on the arrestee's person. Id. at 2488. The question in Riley, then, was not whether accessing the data constituted a search, but whether that search constituted such an intrusion into an arrestee's (diminished) expectation of privacy that it fell outside of the search-incident-to-arrest exception. The court concluded that it did, and based that decision on the nature of a cell phone as opposed to the nature of other objects an arrestee might carry (such as wallet). Id. at 2489.

The Court emphasized the "immense storage capacity" of cell phones as opposed to other things a person might carry. Id. The Court found that that storage capacity allowed a person to carry, in one device, "the sum of an individual's private life." Id. The Court also found significant the pervasiveness of cell phones—the Court stated that "it is no exaggeration to say that many of the more that 90% of American adults who own a cell phone keep on their person a digital record of nearly every aspect of their lives—from the mundane to the intimate." Id. at 2490. The Court opined that "[a]llowing the police to scrutinize such records on a routine basis is quite different from allowing them to search a personal item or two in the occasional case." Id. It posited that

> a cell phone search would typically expose to the government fare *more* than the most exhaustive search of a house; A phone not only contains in digital form many sensitive records previously found in the home; it also contains a broad array of private information never found in a home in any form—unless the phone is.

Id. at 2490-91.

The Court also noted that cell phone users could access data stored on remote servers (in the "cloud") when the phone was connected to the internet. Id. at 2491. The government had conceded that data stored in the cloud did not fall within the scope of the search-incident-to-arrest warrant exception, and the Court analogized a search of cloud-stored data from an arrestee's phone to "finding a key in a suspect's pocket and arguing that it allowed law enforcement to unlock and search a house." Id. The Court stated, however, that an officer viewing an arrestee's phone data likely could not know whether she was viewing locally-stored or remotely-stored data, and thus that extending the search-incident-to-arrest exception to allow officers to access phone data would necessarily allow them to access data not stored on the device. Id.

The government argued in the alternative that the Court ought at least extend the search-incident-to-arrest exception to allow officers to search the phone's call log. Id. at 2492. In making this argument, the government relied on the Court's pen-register decision in Smith v. Maryland. The Riley Court rejected this argument, stating: "The Court in [Smith], however, concluded that the use of a pen register was not a 'search' at all under the Fourth Amendment. There is no dispute here that the officers engaged in a search of Wurie's cell phone." Id. at 2492-93 (citations omitted).

The Riley Court concluded, "Our holding, of course, is not that the information on a cell phone is immune from search; it is instead that a warrant is generally required before such a search, even when a cell phone is seized incident to arrest." Id. at 2493. The Court also left room for the possibility that,

while the search-incident-to-arrest exception did not apply to cell phones, "other case-specific exceptions may still justify a warrantless search of a cell phone." Id. at 2494.

Analysis of Graham In Light of Supreme Court's Jurisprudence

As stated earlier, against this backdrop, the defendant urges this court to follow the Fourth Circuit's reasoning in Graham, and to find that when the government obtains cell site location data from the provider, that action constitutes a search for Fourth Amendment purposes. This court is not persuaded by the Graham court's reasoning.

The Graham court first concluded that, "[l]ike the searches challenged in *Karo* and *Kyllo*, examination of historical CSLI can allow the government to place an individual and her personal property—specifically, her cell phone—at the person's home and other private locations at specific points in time." Graham, 796 F.3d at 346. The Graham court combined its reading of Karo (striking down the monitoring of a transmitter inside a private residence) and Kyllo (striking down law enforcement's use of a thermal imaging device to obtain information about heat transmission inside the home) to reach the conclusion that those two courts "recognized the location of a person and her property within a home at a particular time as a 'critical' private detail protected from the government's intrusive use of technology." Id. at 347.

This court does not agree. Neither Karo nor Kyllo stood for the proposition that an individual had a reasonable privacy interest in whether or not she was inside her home. Rather, both cases emphasized a concern that

use of devices such as transmitters and thermal imagers provided law enforcement with details about the interior of an individual's home that they could not have detained via traditional surveillance.

Katz, Knotts, and Jones all acknowledged in different ways that obtaining facts by visual surveillance (of a person, of the travels of a car) did not constitute a search. A well-established investigative tool is the "stake-out," where officers station themselves outside of a location and watch to see who enters and who leaves. Another is a "tail," where officers follow individuals to see where they go, and with whom they meet. Cell phone site data uses electronic means to collect that same information, without the same commitment of law enforcement personnel. As the Knotts Court stated, "nothing in the Fourth Amendment prohibited the police from augmenting the sensory faculties bestowed upon them at birth with such enhancement as science and technology afforded them in this case." Knotts, 460 U.S. at 282.

It is true that the Karo Court disapproved of the government using a device to determine

> [t]hat a particular article is actually located at a particular time in the private residence and is in the possession of the person or persons whose residence is being watched. Even if visual surveillance has revealed that the article to which the beeper is attached has entered the house, the later monitoring not only verifies the officers' observations but also establishes that the article remains on the premises.

Karo, 468 U.S. at 715. The critical distinctions between the activity in Karo and the collection of cell site location data, however, are that (a) in Karo the officers, without the defendant's consent, placed the transmitter in the container which

made its way inside the residence, whereas the defendant in this case chose to purchase, carry and use his phone; and (b) the defendant in Karo did not voluntarily turn the transmitter data over to a third party—this court believes the defendant in this case did, as it will explain.

The Graham court next concluded that, unlike visual surveillance, the government could obtain from cell site location data location information about an individual over long periods of time. This led the court to Jones, and the concerns expressed by concurring justices, such as Justice Sotomayor, that "longer term [electronic] monitoring in investigations of most offenses impinges upon expectations of privacy." Graham, 796 F.3d at 347 (citing Jones, 132 S. Ct. at 955) (Sotomayor, J., concurring). Combining the Jones decision with its reading of Karo and Kyllo, the Graham court concluded that "the government engages in a Fourth Amendment search when it seeks to examine historical CSLI pertaining to an extended time period like 14 or 221 days." Id. at 350.

That conclusion is overly broad. The Jones majority decided that the collection of the GPS data was a search, not because of how long the data collection went on, but because the government trespassed on the defendant's property by installing the device on the car, and leaving it there, without a warrant. Jones, 132 S. Ct. at 952 ("Jones, who possessed the Jeep at the time the Government trespassorily inserted the information-gathering device, is on much different footing [than the defendant in Karo].")

In her concurring opinion, Justice Sotomayor agreed that the GPS tracking constituted a search, but did not agree with the majority that that

conclusion was mandated by the trespass theory. Rather, she concluded that the GPS monitoring violated the defendant's reasonable expectation of privacy. She opined that "[i]n the pre-computer age, the greatest protections of privacy were neither constitutional nor statutory, but practical." Id. at 963. She explained that in that era, law enforcement could not conduct constant surveillance of an individual "for weeks" without a massive expenditure of resources—"a large team of agents, multiple vehicles, and perhaps aerial assistance." Id. Justice Sotomayor concluded that given the practical problems with conducting extended periods of surveillance using non-electronic surveillance methods, "society's expectation has been that law enforcement agents and others would not—and indeed, in the main, simply could not—secretly monitor and catalogue every single movement of an individual's car for a very long period." Id. at 964. In other words, she concluded that individuals had an objectively reasonable expectation of privacy in the history of their whereabouts over time, because they had a reasonable expectation that law enforcement did not have the capability to conduct such long-term surveillance. She concluded that the Court did not need to "identify with precision the point at which the tracking of this vehicle became a search, for the line was surely crossed before the 4-week mark." Id.

This court disagrees that today, when many Americans own some sort of cell phone and carry it frequently, an individual's expectation that the government could not track his whereabouts over time is reasonable. The media is rife with information—and sometimes warnings—about the fact that

one's location can be tracked from one's cell phone. There are web sites that claim to allow one to "find the exact location of any phone." Kim Komando, Find the Exact Location of Any Phone (May 31, 2014), www.domando.com/tips/2553377/find-the-exact-location-of-any-phone/all. There are applications that purport to allow family members to track each other's locations through their phones. LIFE360, https://www.life360.com, last checked March 11, 2016. There are web sites that purport to teach viewers to track cell phone locations using applications not necessarily created for that purpose. Ryan Dube, How to Trace a Mobile Phone Location with Google Latitude, MAKEUSEOF, (May 22, 2009), www.makeuseof.com/tag/how-to-trace-a-mobile-phone-location-with-google-latitude/. There are articles warning that applications on one's smart phone collect location data. Bob Sullivan, A Shock In the Dark: Flashlight App Tracks Your Location, NBC NEWS, (Jan. 16, 2013, 6:06 a.m.), www.nbcnews.com/business/consumer/shock-dark-flashlight-app-tracks-your-location-f1B7991120. Many smart phone applications politely ask phone owners for permission to use their locations in order to map travel routes (Google Maps), find restaurants (Yelp, Foursquare), or locate the cheapest gas at stations nearby (GasBuddy).

Popular culture promotes the notion that the government, too, can determine extensive information about an individual from, among other things, one's phone. In 2013, the news was filled with former National Security Agency contractor Edward Snowden's revelations regarding the extent to which the NSA allegedly was collecting phone metadata without warrants or court orders;

controversy continues regarding whether such a practice was justified, necessary or lawful. See, e.g., Catherine Treyz, NSA Ends Bulk Phone Data Collection, CNN, (Nov. 28, 2015, 6:57 p.m.), http://www.cnn.com/2015/11/28/us/nsa-ends-bulk-phone-surveillance/. As long ago as 2004, the popular HBO series "The Wire" devoted an episode to the use of the disposable prepaid cell phones used by the drug-dealing characters in the show. THE WIRE, 32: BACK BURNERS (HBO 2004), available at http://www.hbo.com/the-wire/episodes/3/32-back-burners/index.html. In 2008, the Seventh Circuit referenced the show in noting that "prepaid cellular phone[s] with no subscriber information," known as "dope phones" or "burners" were "difficult to trace and a favored tool of drug dealers." United States v. Fiasche, 520 F.3d 694, 695 and n.1 (7th Cir. 2008). A common plot mechanism in police and crime shows involves officers using triangulation techniques to locate someone via their cell phone.

The court points to the abundance of exposure the concept has had because, given that abundance, it is becoming more and more unlikely that an individual's expectation that the government could not track his location for an extended period of time, "viewed objectively, is 'justifiable' under the circumstances." Knotts, 460 U.S. at 281 (citing Katz, 389 U.S. at 351)). For these reasons, the court does not agree with the Graham court that the government invades a "reasonable" expectation of privacy "when it relies upon

technology not in general use to discover the movements of an individual over an extended period of time." Graham, 796 F.3d at 349.[5]

The Graham court also disagreed with the government that its activity was not a search because the government obtained the cell site location data from a third party. Id. at 353. The court held that a cell phone user did not voluntarily turn cell site data over to a third-party provider. The court stated, "We decline to apply the third-party doctrine in the present case because a cell phone user does not 'convey' CSLI to her service provider at all—voluntarily or otherwise—and therefore does not assume any risk of disclosure to law enforcement." Id. at 354. It explained this conclusion as follows:

> The service provider automatically generates CSLI in response to connections made between the cell phone and the provider's network, with and without the user's active participation. . . . . "Unlike the bank records in *Miller* or the phone numbers dialed in *Smith*, cell-site data is neither tangible nor visible to a cell phone user." *In re Application of U.S. for Historical Cell Site Data*, 747 F. Supp. 2d 827, 844 (S.D. Tex. 2010), *vacated*, 724 F.3d 600 (5th Cir. 2013). A user is not required to actively submit any location-identifying information when making a call or sending a message. Such information is rather "quietly and automatically calculated by the network, without unusual or overt intervention that might be detected by the target user." *Id.* at 833. We cannot impute to a cell phone user the risk

[5] The officers in Jones collected cell site location data for twenty-eight days. Jones, 132 S. Ct. at 948. In this case, the government obtained thirty days' worth of cell site location data. Dkt. No. 9-1 at 10. In Graham, the government collected 221 days' worth of data. Graham, 796 F.3d at 347. Like Justice Sotomayor, this court makes no determination regarding whether, and when, a cell phone user's expectation of privacy might become more reasonable due to the number of days' worth of data the government collects. For the reasons stated above, the court finds that the defendant did not have a reasonable expectation that the government could not determine his whereabouts over a thirty-day period.

> that information about her location created by her service provider will be disclosed to law enforcement when she herself has not actively disclosed this information.

Id. at 354-55 (some citations and internal quotations omitted).[6]

The Graham court rejected the Fifth Circuit's conclusion that "users know that they convey information about their location to their service providers when they make a call." Id. at 355 (quoting U.S. for Historical Cell Site Data (In re Application (Fifth Circuit)), 724 F.3d at 612). The Graham court held that "[p]eople cannot be deemed to have volunteered to forfeit expectations of privacy by simply seeking active participation in society through use of their cell phones." Id. at 356. The court found that the question was not whether users understood generally how their cell phones worked, but rather, "whether users are generally aware of what specific cell sites are utilized when their phones connect to a cellular network. . . . We have no reason to suppose that users generally know what cell sites transmit their communications or whether those cell sites are located." Id.

[6] The Graham court also found relevant that its case involved location information, "not only for those transmissions in which Appellants actively participated—i.e., messages or calls they made or answered—but also for messages and calls their phones received but they did not answer." Graham, 796 F.3d at 355. It concerned the Graham court that with this information, "the phone's location is identified without any affirmative act by its user at all—much less, 'voluntary conveyance.'" Id. (citations and internal quotes omitted). As indicated in footnote 1 above, the government has indicated to the defense in this case that it plans to use only cell tower data—identified in the attachment to the court order as "[a]ll data about which 'cell towers' (i.e., antenna towers covering specific geographic areas) and 'sectors' (i.e., faces of the towers) received a radio signal from each cellular telephone or device assigned to the account." Dkt. No. 9-1 at 11. It does not appear to the court, from this description, that the information the government seeks to use in this case is as broad as that the government sought to obtain in Graham, and thus will not discuss this portion of the Graham decision.

This court finds the Graham court's rationale hard to square with the Supreme Court's decisions regarding the third-party doctrine. Each of the third-party doctrine cases this court discussed above involved situations in which a user chose to utilize a modern convenience, and by so choosing, exposed information about himself to a third party. A person chooses to put money in a bank—whether because it is safer, or more convenient, or provides interest income—but that is a choice. That same person could keep his money at home in a mattress, and avoid the risk that the bank will share his financial information with law enforcement. A person chooses to put his household garbage into a bin and set it out by the curb for collection, in lieu of composting it in his back yard or taking it somewhere to burn. The latter actions, while messy and inconvenient, would avoid the risk that the sanitation department will share what's in that garbage with law enforcement. A person chooses to use a telephone, when she could communicate by letter or by visiting the person with whom she wishes to speak, but that choice puts her at risk that the phone company will disclose information about her to law enforcement.

It is not practical to assume in 2016 that the majority of people will live their busy, interconnected and global lives without using banks, garbage collection, credit cards, telephones, but the Supreme Court's third-party doctrine decisions do not analyze whether it would be difficult for an individual to function without those conveniences. They analyze whether it is reasonable for that individual to expect that once she utilizes a particular convenience, the

third party who collects the trail of information that use leaves behind will not share it with law enforcement.

This court also is puzzled by the Graham court's assertion that an individual has a reasonable expectation of privacy in cell tower data because she does not know which cell towers transmit the communications, or where they are located. Cell users know that they need to be in some sort of proximity to a tower in order to have cellular service. Those who drive specific routes each day to work know well the spots where they're likely to lose service, and where they will regain it. Subway riders know why they lose service when they enter the tunnels. Perhaps cell users do not know, at the moment they discover that they have reception, where the tower is located. But users of cell phones know, at all times, that if their phone is connected to a network, they're in some kind of proximity to a tower, and that if it is not connected, they likely aren't.

In sum, this court does not agree with the Graham court that a cell phone user has a *reasonable* expectation that the government cannot track his location via his phone.

Conclusion

The court concludes that the government's collection of cell tower location data from the cell phone provider does not constitute a "search" under the Fourth Amendment. The collection of the data does not involve a trespass upon an individual's person or property, nor into a physical area in which the person has established a reasonable expectation of privacy. Individuals do not

have a reasonable expectation that they may use their cell phones to make and receive calls and yet have their location remain private. Because the collection of this data does not constitute a search, the government did not violate the Fourth Amendment by obtaining the defendant's cell tower location data by means of a court order, rather than by obtaining the SCA-authorized order.

The court **ORDERS** that the defendant's December 4, 2015 motion to suppress evidence is **DENIED**. (Dkt. No. 9)

Dated in Milwaukee, Wisconsin this 14th day of March .

BY THE COURT:

HON. PAMELA PEPPER
United States District Judge